

# **MINUTES OF THE COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD MEETING**

**DECEMBER 10-12, 1996**

**Tuesday, December 10, 1996**

## **Introduction**

A quorum being present, Dr. Willis Ware, Board Chairman, called the meeting to order at 9:00 a.m. In addition to Dr. Ware, the following Board members were present: Genevieve Burns, John Layton, Joe Leo, Gloria Parker, Randy Sanovic and Linda Vetter. Mr. Charlie Baggett arrived later in the afternoon; additionally, Mr. George Spix was in attendance on Thursday, December 12.

Mr. Ed Roback, Board Executive Secretary, welcomed the members and reviewed the agenda and handout materials for the three-day meeting. He reported on the status of existing Board vacancies: one candidate had been tentatively identified and the lengthy process of obtaining official clearances has been initiated. Mr. Roback said that it would be useful if members would provide him with names of additional individuals for consideration for the remaining vacancy (in the computer/ telecommunications industry expert category).

Chairman Ware mentioned a recent article that had appeared in the *Los Angeles Times* that dealt with the subject of the state of computer security in the federal government. It was broad in scope but specifically addressed the Social Security Administration and the Internal Revenue Service. He put it on the table for the Board to decide if they could do anything about this issue.

## **Update on Activities of the Presidential Commission on Critical Infrastructure Protection (PCCIP)**

Mr. William Joyce, a newly appointed member of the PCCIP originally from the Central Intelligence Agency, addressed the Board on the PCCIP's current activities. Since the PCCIP's last briefing to the Board in September, the Commission is still in the process of completing the appointments of the Chairman and the Steering Committee. The selection of the private sector advisory committee and private sector commissioners has not yet been formally announced. The Commission has focused on vulnerability and threat reviews and consultations with public and private sector stakeholders have been held. To date, they have conducted a review of the rail industry critical infrastructure and consider themselves in the data-gathering stage. Thus far, the initial assessments include: lack of U.S. government consensus on threat dimensions; limited buy-in from the private sector; incomplete vulnerability analysis, and lack of integration of the indications and warning process. Even given the tight deadline for accomplishing their tasks, it

is the consensus of the Commission to focus all eight infrastructure areas. Mr. Joyce said that the Commission hopes to have a world wide web site in place just as soon as the official announcement is made by the White House. (See Reference #1)

### **Infrastructure Protection Task Force (IPTF) Activities, PCCIP**

Mr. John McClurg, Unit Chief, described the IPTF's mission to protect the national infrastructures against both physical and cyber threats. The IPTF's principal tasking is to identify and coordinate existing expertise in and out of government. As an operational entity, the IPTF has five sub-tasks: 1) identify and coordinate to detect, prevent, halt, confine and recover; 2) coordinate issuance of threats and warnings; 3) provide training and education to reduce vulnerabilities and to respond to attacks; 4) conduct after-action analysis; and, 5) coordinate attacks with appropriate law enforcement agencies. It will not supplant existing programs or organizations. Current major players include: FBI, CIA, DOD, NSA, DOE, DOT, DIA, FEMA, NCS, NIST, Treasury, DOJ and the private sector.

This activity is physically located at the FBI Headquarters; it is co-located with the Computer Investigations and Infrastructure Threat Assessment Center (CITAC). There are three regional computer crime squads now in place; Washington, DC; San Francisco, CA and New York, NY. Other are being formed in 56 field offices. Working together they assist in vulnerability identification and mitigation; provide national and international prospective; assess possible coordinated attacks and identify interdependencies across infrastructures. (See Reference #2)

### **Update on Key Management Infrastructure Program**

Patty Edfors briefed the Board on the Federal Public Key Infrastructure activities. She reviewed the vision, approach and objectives of the program. Their current course of action included bringing NIST, NSA, GSA, DOD, GITS, FNC and OMB together to discuss necessary attributes of a PKI; addressing GAO requirements for federal obligations; meeting with agencies, states and industry to discuss requirements/projects; working with IT Fund subgroup, GITS, IMC and others to integrate projects wherever possible; implement the Root Certificate Authority (CA) function to determine interoperability requirements and the necessity of a Root CA. She concluded her presentation by stating that a considerable amount of coordination is necessary; a business case must be made for the use of this technology; testing the original studies to determine applicability and that interconnectivity and interoperability are critical. (See Reference #3)

### **Update on Administration Crypto Issues and Status Report of the Technical Advisory Committee to Develop a FIPS for the Federal Key Management Infrastructure**

Ed Roback stated that since our last briefing by Bruce McConnell of OMB, the Administration has announced its intent to allow firms to export DES without key recovery, provided they submit a plan to migrate toward the provision of key recovery products over a two year period. This will be codified in regulations expected to be issued before the start of the new year.

With regard to activities of the OECD, a meeting will be held in Paris the week of December 13<sup>th</sup> to complete Committee work on the draft cryptography principles. It is expected that the final touches will be made to the proposed draft guidelines for forwarding to the parent committee for approval. Mr. Roback, who will attend as a member of the U.S. delegation, stated he would update the Board on these activities in March.

Mr. Roback also noted that there had been recent press reports on the possibility of NIST starting a program to come up with a new standard in the area of encryption. NIST is considering such a proposal and would work closely industry and voluntary standards groups to identify a suitable candidate(s) for a new standard. The large installed base of DES products and that DES will continue to be of sufficient strength for many applications. Migrating toward a new standard will involve a lengthy transition process. SKIPJACK, a classified algorithm, will not be the new standard. A formal announcement of this effort is expected in the near future.

Mr. Roback reported on the newly established Technical Advisory Committee to Develop a Federal Information Processing Standard for the Federal Key Management Infrastructure. Officially chartered in July 1996, the mission of this Committee is to get industry's advice on writing a key recovery federal standard. The Committee is working the key recovery problem for confidentiality of encryption keys only. There are 24 members drawn from industry and the university community, as well as 10 federal agency [non-voting] liaisons. The first meeting was held December 5 and 6 in Dallas and was opened by Department of Commerce Under Secretary for Technology, Dr. Mary L. Good. Working groups will be formed and six additional meetings are being planned for next year. The goal of the first year is to develop the framework for the standards followed by more technically detailed recommendations..

## **Privacy Issues Update**

Mr. Marc Rotenberg, Director of the Electronic Privacy Information Center, presented a privacy issues update. He reviewed the results of a recent Internet privacy poll that was conducted by the Georgia Institute of Technology. The results indicated that users were most concerned about censorship, privacy and navigation issues.

The Administration is still studying the privacy problem. He pointed to several studies [Federal Trade Commission, National Telecommunication and Information Administration, Federal Reserve Board and the Ira Magaziner report on e-commerce]. The areas that Congress is like to act on cover privacy of children, medical privacy, privacy commission and Internet privacy.

He reported on a new German Telecommunications bill. He highlighted its high points and indicated that it is expected to be well received by other countries and probably adopted by them as well.

With regard to the OECD activities, he stated that the next meeting in Paris will draw closer to finishing the development of the international guidelines for cryptography. They have a sensible policy framework of eight central principles. He stated that the U.S. position is incoherent and lacks support. The primary focus of the OECD is promotion of economic growth.

Mr. Rotenberg went on to discuss the crypto issues in Congress. He said that Congress was displeased with the recent Executive Order (transferring jurisdiction of export control administration from the Department of State to the Department of Commerce) and that a revised crypto bill is likely. He expects multiple dimensions of debate to take place within this next Congressional year between industry versus government, privacy versus surveillance, and Congress versus the President.

He discussed the current activities in the Courts involving crypto issues on the following cases: *Karn v. State*; *Bernstein v. U.S.*; and *Junger v. State*. He also briefed on the issue of censorship in cyberspace surrounding the Supreme Courts agreement to hear the case, *ACLU v. Reno*. (See Reference #4)

## **Discussion Period**

The Board set aside this time to review and discuss issues for the development of a work plan for 1997 and beyond. Highlights included:

- (1) keep abreast of the possibility of the Administration establishing a privacy@ office and the possibility of developing recommendations for their consideration;
- (2) keep abreast of all new privacy legislation issues; invite staff to address the Board on pending activities in this area;
- (3) examine the proliferation of government databases that are being mandated by recent legislation; offer to be a forum where issues that are being polarized can be presented and possibly resolved;
- (4) find out who has the overall responsibility for government privacy and obtain their interpretation of the Privacy Act;
- (5) need for identification of what the collected databases will do as far as threats and problems are concerned; need to ask the database collectors to brief the Board on what threats they see;

- (6) need to be proactive; raise issues; find out who has ownership; what their status is, and if they are going in the right direction; offer support if they are or suggest another direction, if necessary;
- (7) ask privacy advocates or technical experts who should be invited in to discuss these issues; technologists could be asked to give their thoughts on the future and where we are headed;
- (8) develop a set of questions that would cover our concerns;
- (9) ask agencies with already established databases, such as the IRS or SSA, to discuss their activities especially with regard to privacy; and
- (10) focus on additional issues (i.e., electronic commerce; digital signature and identification arena activities).

### **Wednesday, December 11, 1996**

#### **Public Key Infrastructure - General Overview**

Mr. Noel Nazario of NIST's Computer Security Division, presented a general overview of the public key infrastructure. NIST has a PKI team working with other organizations both within and outside of the government. Mr. Nazario covered the working definition and challenges involving certification authority structures, subject identification, key and certificate life cycle management, revocation, policies, constraints and authorization information. (See Reference #5)

#### **Federal PKI Legal Policy Working Group**

Allen Church of GSA represented this recently established working group, one of three under the Federal PKI Steering Committee (chartered under the GITS Board) which shares information with CIO Council, NPR and OMB. Interagency efforts include working with SSA, GSA, DOJ, PTO, DOE, NTIS, IRS, NSA, DOT, NIST, USPS, NASA. Topics of concern include: digital and electronic signatures; evidentiary value of these signatures; policies assuring the authenticity of holders of public key certificates; role of FIPS in a public key infrastructure; key/data recovery issues; and legal status with regard to criminal prosecutions. He reported on their current progress and future issues. (See Reference #6)

#### **CommerceNet**

Mr. Bob Daniels of SSA presented an overview of the CommerceNet involvement in the PKI effort. CommerceNet is a non-profit organization and consortium with projects to define business models; develop tools for evaluating certificates and CRLS; develop boilerplate CPS; develop sample agreements for EC; define assurance levels; and develop insurance guidelines. They see a strong business case in moving with a PKI infrastructure and see their biggest hurdle as developing acceptable authentication standards.

## **PKI Pilots**

Mr. Daniels also briefed on the SSA pilot project. SSA has established an electronic service industry steering committee team to develop ideas to provide better service to the public. They are working on three pilot programs involving use of the Internet. One involves obtaining personal earning and estimated benefits information over the net. Since April, there have been over 50,000 requests via this method and this has been done without advertising. There is a savings of \$1.50 for every request that is done via on-line. The other two areas of involvement are 1) certificate of coverage of social services taxes to be used by Americans employed overseas to make sure that social services taxes are only paid to the U.S. and not to the foreign country the employee may be working in, and 2) work involving electronic W2/W3 forms. This latter pilot is the first real time digital signature applications in the government and currently uses a software developed by Pitney Bowes that allows W2s to be submitted on-line and provide a printed out paper copy as well. It is expected that Form 1099s will be available on-line in January; however, they are not expected to use digital signatures.

The next presenter was Mr. Don Heckman of the National Security Agency who briefed on their MISSI Security Management Infrastructure (SMI). This program provides key and certificate management services so that applications making use of the FORTEZZA crypto cards can provide the desired security services. Mr. Heckman covered the concept of operations, an overview of the target SMI, its hierarchy, CA registration process, documentation and components. He also discussed the current and future development activities. (See Reference #7)

Ms. Donna Dodson of the NIST Computer Security Division presented a briefing on NIST's minimum interoperability specifications for PKI components (MISPC). She stated that the goal of this effort is to work with industry through Cooperative Research and Development Agreements (CRADAs) to develop a specification for interoperable COTS PKI products which support commercial and government designs and interoperable private sector and government PKIs. Current CRADA partners include: AT&T, BBN, CertiCom, Cylink, DynCorp, IRE, Motorola, Northern Telecom, SpyruS, and VeriSign. A draft version 1 of the specifications is expected to be available to the public for review and comment this month. Ms. Dodson solicited comments from the Board. (See Reference #8)

## **Intellectual Property Issues**

Mr. Peter Jaszi, a law professor at American University, discussed the intellectual property (IP) issues regarding copyright in the digital network environment. Mr. Jaszi is a member of a digital futures coalition covering both the international and national IP issues. He reported that Bruce Lehman, Director of the Patent and Trademark Office, chaired an IP rights working group established under the NII program. This working group was charged with examining the full range of domestic IP laws and making a report on the context of existing law suggestions for law reform. The bulk of this report dealt with copyright issues. The resulting report contained two components: 1) a narrative to describe the ways in which existing intellectual law applies in the digital environment, and 2) a set of draft legislative recommendations for revisions to Title 17, the Copyright Act. This proposal was incorporated into legislation introduced in the last Congress (HR2241, S1284).

On the international side, the Berne Convention of Literature Arts convenes approximately every 20 years to conduct formal meetings on the world IP issues and possibilities for revisions. Since the last convention in 1991, it had become clear that it would be difficult to have another general conference because of the many issues of the copyright subject. Six and one-half years ago the World Intellectual Property Organization (WIPO) began to hold a series of experts meetings to do preparatory work leading to conventions that would produce supplementary treaties on intellectual property. However, when the United States wanted to add the digital agenda to the next diplomatic conference scheduled for December 1996 in Geneva, this resulted in strong objections from the educational community, the library community, from significant parts of hardware manufacturers, consumers and electronic privacy groups.

Mr. Andrew Grosso, an attorney for the Association for Computing, expressed their concerns, in particular those regarding the downloading of documents into RAM. He reviewed the fine lines that exist between copyright-ability of diagnostic downloadable software versus browsing activities on the Internet.

### **National Research Council Health Care Report**

Mr. Jerry Sheehan presented an interim status report on an NRC committee's project involving improving the security of electronic health information. This project was sponsored by the National Library of Medicine with support from the Massachusetts Health Data Consortium. The charge to the group was: to observe and assess mechanisms for protection privacy and maintaining security in health care information systems; identify other methods worthy of testing in health care settings; and outline promising areas for further research and development. Mr. Sheehan described the committee membership and discussed the six site visits that had taken place. He reviewed the topics discussed at this site visits and identified the information technology that existed within them. The interim report describes the practices of the organizations for protecting their sensitive medical records. (See Reference #9)

**Thursday, December 12, 1996**

The morning session of this meeting was devoted to a series of briefings from the Department of Agriculture on how they are dealing with privacy issues and their programs.

### **Recent Legislative Initiatives for IT**

Mr. Joe Leo, Board Member, reviewed sections of the Personal Responsibility and Work Opportunity Reconciliation Act of 1996 that cover the provisions to encourage electronic benefit transfer and the development of prototype of counterfeit-resistant Social Security cards.

### **Food and Consumer Service EBT Status Report**

Mr. Jerry Cohen gave a briefing on the provisions within the Personal Responsibility and Work Opportunity Reconciliation Act of 1996. He reviewed the current provisions and the new provisions of this legislation.

### **OIG 's Perspective on EBT Security**

Next, Mr. James Ebbitt, Assistant Inspector General, Audits, Office of the Inspector General (OIG), USDA, began his presentation with an overview of the OIG, covering the staff and fiscal overview. They conduct audits and investigations, oversight audits and investigations, provide recommendations, receive employee complaints, report violations of law to Justice, review legislation and regulations and inform the Secretary of Agriculture and the Congress. They do not manage programs or establish policy. They are EBT partners with federal agencies and state governments, as well as those in the private sector such as financial institutions and processing companies.

### **Update on EBT Security Demonstration Project**

Mr. John Donovan ' s presentation covered EBT security systems. He reviewed the security controls in place in each of the components. He also presented a geographical review of the food stamp program ' s EBT development throughout the United States.

### **FCS Perspective on Biometrics - Finger Imaging**

Mr. Cohen addressed the food and consumer service perspective on use of biometric technology an anti-fraud tool. He stated that several States are in the process of developing projects to pilot test the use of biometric technology applications, such as finger imaging. Other States are using retinal scan, iris scan, voice recognition, and electronic signature as biometric techniques.

Mr. Leo provided a summary/wrap-up of the presentations. This was followed by dialogue with the Board. (See Reference #10)

### **Future Agenda Planning**

The board passed a resolution to examine the efforts of new information technology and government information practices on privacy. (See Attachment #1.) In this resolution, the Board stated that there had been many changes in the 22 years since fundamental legal protections for information privacy were established under the Privacy Act of 1974. They solicited input from the public in order to be better informed and can make appropriate recommendations in accordance with their mission. The Board also directed the Chairman to write a letter to the head of the Government Information Technology Services, James Flyzik, conveying the Board's commendations for the efforts of and presentations by Patricia Edfors, GITS spokesperson, in the area of PKI.

The Board identified areas of interest for future agendas. They discussed the possibility of dedicating the June meeting to privacy topics and suggested calling for written material in advance from which presentations could be considered. Other areas mentioned included privacy and security issues relating to the student loan program; privacy issues of airline travelers; OMB's vision of implementing the National Performance Review's policy of security and privacy.

There being no further business, the meeting was adjourned at 3:00 p.m.

Attachment:

Resolution 96-2

References:

- #1 - Joyce slides
- #2 - McClurg slides
- #3 - Edfors slides
- #4 - Rotenberg slides
- #5 - Nazario slides
- #6 - Church slides
- #7 - Heckman slides
- #8 - Dodson slides
- #9 - Sheehan slides
- #10 - Department of Agriculture handouts

Edward Roback  
Executive Secretary

CERTIFIED as a true and  
accurate summary of the  
meeting

Willis H. Ware

Chairman